

GAO

Report to the Secretary of the Treasury

September 2000

FINANCIAL MANAGEMENT SERVICE

Significant Weaknesses in Computer Controls



DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited



G A O

Accountability * Integrity * Reliability

GAO/AIMD-00-305

DTIC QUALITY INSPECTED 4

20000929 004



United States General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-286258

September 26, 2000

The Honorable Lawrence H. Summers
The Secretary of the Treasury

Dear Mr. Secretary:

In connection with fulfilling our requirement to audit the U.S. government's fiscal year 1999 financial statements,¹ we reviewed the general and application computer controls over key financial systems maintained and operated by the Department of the Treasury's Financial Management Service (FMS). These systems, some of which are operated and maintained by contractors and the Federal Reserve Banks (FRB), are critical to FMS' mission of serving as the government's financial manager, central disburser, collections agent, and reporter of financial information. On September 22, 2000, we issued a Limited Official Use report to you detailing the results of our review. This excerpted version of the report for public release summarizes (1) the significant weaknesses we identified and recommendations we made and (2) our follow-up on previously reported weaknesses.

Our fiscal year 1999 tests of the effectiveness of general and application controls that support key FMS systems identified computer control weaknesses that place FMS' financial systems at significant risk of fraud, unauthorized disclosure and modification of sensitive data and programs, misuse or damage to computer resources, or disruption of critical operations. We followed up on the status of FMS' corrective actions to address weaknesses discussed in our fiscal year 1998 report.² Our follow-up work found that many of the weaknesses we discussed in our fiscal year 1998 report³ continued during fiscal year 1999. While performing our work, we communicated detailed information regarding our findings to FMS management. This report provides an overall assessment and summary of

¹31 U.S.C. 331(e) (1994).

²*Financial Management Service: Significant Weaknesses in Computer Controls* (GAO/AIMD-00-04, October 4, 1999).

³The weaknesses discussed in our fiscal year 1997 report that remained unresolved at September 30, 1998, were carried forward and reported in our fiscal year 1998 report.

FMS computer control weaknesses and recommendations to you as the agency head.

We also assessed the general and application computer controls over key FMS systems that the FRBs maintain and operate and have issued a separate report to the Board of Governors of the Federal Reserve System.⁴

Results in Brief

The pervasive weaknesses we identified in FMS' computer controls at most of its data centers during our fiscal year 1999 audit render FMS' overall security control environment ineffective in identifying, deterring, and responding to computer control weaknesses promptly. Consequently, billions of dollars of payments and collections are at significant risk of loss or fraud, sensitive data are at risk of inappropriate disclosure, and critical computer-based operations are vulnerable to serious disruptions. As we reported for fiscal years 1998 and 1997, we consider FMS' computer control problems a material weakness.⁵ FMS officials have also recognized the serious nature of these problems and have reported these matters as a material weakness in its Federal Managers' Financial Integrity Act (FMFIA) report for fiscal years 1999 and 1998.

During our fiscal year 1999 audit, we found new general computer control weaknesses in access controls, system software, and segregation of duties. We also identified new weaknesses in the authorization controls over two key FMS financial applications. Our follow-up on the status of FMS' corrective actions to address weaknesses discussed in our fiscal year 1998 report found that as of September 30, 1999, FMS had corrected or mitigated the risks associated with 52 of the 94 computer control weaknesses discussed in that report. To assist FMS management in addressing its general computer control weaknesses, the Limited Official Use version of this report contained 59 detailed recommendations.

In commenting on a draft of this report and our more detailed Limited Official Use report, FMS stated that its general and application security

⁴*Federal Reserve Banks: Areas for Improvement in Computer Controls* (GAO/AIMD-00-218, July 7, 2000).

⁵A material weakness is a condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that errors or irregularities in amounts that would be material to the financial statements may occur and not be detected promptly by employees in the normal course of performing their duties.

controls must continue to be improved. FMS also stated that it has taken and will continue to take actions to correct the weaknesses we identified.

Background

FMS is the government's financial manager, central disburser, and collections agency as well as its accountant and reporter of financial information. For fiscal year 1999, the U.S. government disbursed over \$1.7 trillion primarily for Social Security and veterans benefit payments, Internal Revenue Service (IRS) tax refunds, federal employee salaries, and vendor billings. With several exceptions (the largest being the Department of Defense), FMS makes disbursements for most federal agencies. FMS is also responsible for administering the federal government's collections system. In fiscal year 1999, the government collected over \$1.8 trillion from sources such as individual and corporate income tax deposits, customs duties, loan repayments, fines, and proceeds from leases. In addition, FMS oversees the federal government's central accounting and reporting systems used to reconcile and keep track of the federal government's assets and liabilities. Financial and budget execution information from these central systems is used by FMS to publish financial reports that are available for use by the Congress, the Office of Management and Budget, other federal agencies, and others who make financial decisions on behalf of the U.S. government.

FMS maintains multiple financial and information systems to help it process and reconcile moneys disbursed and collected by the various government agencies. These banking, collection, and disbursement systems are also used to process agency transactions, record relevant data, transfer funds to/from the Treasury, and facilitate the reconciliation of those transactions. FMS has three data centers and three field operation centers that are responsible for issuing paper check and electronic funds transfer payments. In addition, FMS relies on three contractor data centers and the FRBs to help carry out its financial management responsibilities.

Objectives, Scope, and Methodology

Our objectives were to evaluate and test the effectiveness of the computer controls over FMS' key financial management systems and to determine the status of the computer control weaknesses discussed in our fiscal year 1998 audit report. We used a risk-based and rotation approach for testing general and application controls. Under that methodology, every 3 years, each data center and key application is subjected to a full scope review that includes testing in all of the computer control areas defined in our *Federal*

*Information Systems Controls Audit Manual (FISCAM).*⁶ During the interim years, we focus our testing on FISCAM areas that we have determined to be at greater risk for computer control weaknesses. See appendix I for the scope and methodology of our fiscal year 1999 review at each of the selected data centers and for the key applications.

During the course of our work, we communicated our findings to FMS management, which informed us of the corrective actions FMS planned or had taken to address the weaknesses we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 2000 financial statements.

We performed our work in accordance with generally accepted government auditing standards from July 1999 through February 2000. We requested comments on a draft of this report from the Department of the Treasury. Its comments are discussed in the "Agency Comments" section of this report and reprinted in appendix II.

FMS' Entitywide Security Management Program Continues to Be Ineffective

An entitywide program for security management is the foundation of an entity's security control structure and should establish a framework for continual (1) risk assessments, (2) development and implementation of effective security procedures, and (3) monitoring and evaluation of the effectiveness of security procedures. A well-designed entitywide security management program helps to ensure that security controls are adequate, properly implemented, and applied consistently across the entity and that responsibilities for security are clearly understood. Our May 1998 best practices guide⁷ on information security management practices at leading nonfederal organizations found that organizations successfully managed their information security risks through an ongoing cycle of risk management activities.

As we discussed in our fiscal year 1998 and 1997 reports, the overriding reason that computer control problems still continued to exist during fiscal year 1999 at FMS was because FMS does not yet have an effective entitywide computer security management program. The lack of an

⁶GAO/AIMD-12.19.6, January 1999.

⁷*Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

effective security management program exposes FMS to the risk that general control weaknesses could occur and not be detected promptly to prevent unnecessary losses or disruptions. FMS' entitywide security control structure has failed to address many of the weaknesses and related significant risks associated with its current and evolving computing environment. Our audits for fiscal years 1999, 1998, and 1997 have identified significant general computer control weaknesses at each of the FMS data centers. As shown in table 1, these weaknesses involved each of the six general control areas defined in FISCAM at multiple FMS data centers.

Table 1: Areas Where Significant General Control Weaknesses Were Identified at FMS Data Centers

Data center	Entitywide security management program	Access controls	System software	Application software development and change controls	Segregation of duties	Service continuity
Fiscal year 1997						
1	X	X	X	X	X	X
2	X	X			X	X
3		X		X	X	X
4		X	X	X		
5		X		X		X
6	X	X	X	X		X
7	X	X		X		X
Fiscal year 1998						
1	X	X	X	X	X	X
2	X	X			X	X
3		X		X		X
4		X	X	X		
5		X		X		
6	X	X	X	X		X
7	X	X	X	X		X
Fiscal year 1999^a						
1	X	X	X	X	X	X
2		X		X		
3		X			X	
4		X				
5	X	X	X	X		
6	X	X				

^aThe payment systems at one of FMS' regional operations centers were moved to a new operating environment at another regional operations center, which mitigated the weaknesses previously identified at the one regional operations center, which are therefore considered closed.

Source: GAO's analysis of current and prior year audit results.

One of the most fundamental elements of an effective entitywide security management program is a current and comprehensive entitywide security policy to communicate security management plans, standards, regulations, or guidelines. An entitywide security policy provides the foundation for a computer security program and helps management ensure that computer controls are working and are reliable, established policies and procedures

are followed, identified deficiencies are promptly corrected, and errors or fraudulent transactions are promptly detected.

In response to our prior year recommendation, FMS officials approved and issued its information security policies in March 2000, which FMS designed to provide overall guidance for the implementation and documentation of its information technology security controls. In addition, a security program manual, guidelines, and end user handbooks are under development, which will provide the detailed security control procedures. According to FMS officials, these documents will be completed in the summer 2000. However, until the related policies and procedures are fully implemented, FMS is at significant risk that responsibilities may not be clear, understood, or properly implemented and security control techniques may not be effectively used or consistently applied.

While FMS is making progress in establishing security procedures and guidance, FMS' approach to security management continues to lack

- adequate site specific written policies and procedures to ensure security administration roles and responsibilities are clearly defined and communicated and that procedures are comprehensive and appropriate for the particular computing environment;
- management enforcement of established security policies and procedures, such as consistently completing background investigations and security violation monitoring and follow-up;
- adequate training of the data center security administrators to ensure security techniques and parameters are properly administered and applied; and
- management enforcement of compliance with certain established standard operating procedures.

Serious General Computer Control Weaknesses Place FMS Systems and Data at Significant Risk

General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. General controls establish the environment in which application systems and controls operate. They include an entitywide security management program, access controls, system software controls, application software development and change controls, segregation of duties, and service continuity controls. An effective general control environment would (1) ensure that an adequate computer security management program is in place, (2) protect data, files, and programs from unauthorized access, modification, and destruction, (3) limit and monitor access to programs and files that control computer

hardware and secure applications, (4) prevent the introduction of unauthorized changes to systems and applications software, (5) prevent any one individual from controlling key aspects of computer-related operations, and (6) ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption.

Our fiscal year 1999 review of FMS' general computer controls identified serious new general control weaknesses in access controls, system software, and segregation of duties. Our follow-up on the status of FMS' actions to correct weaknesses discussed in our fiscal year 1998 report found that FMS completed the migration of one regional operations center's payment systems to a new operating environment at another regional operations center, which mitigated the weaknesses previously identified. Therefore, the weaknesses we identified at the one regional operations center are considered closed.

In addition, as we previously reported for fiscal year 1998, FMS is continuing the process of moving one of its key applications to a distributed environment. FMS officials stated that the migration of all the modules in this key application should be completed in 2001. FMS officials have informed us that they expect the migration to facilitate the implementation of more effective controls in the future.

Our fiscal year 1999 audit found that FMS had corrected or mitigated the risks associated with 52 of the 94 computer control weaknesses discussed in our prior year report. However, we are continuing to reaffirm our prior year recommendations to correct the remaining weaknesses discussed in our fiscal year 1998 report because of the significance of the associated risks and the lack of other effective compensating controls to mitigate those risks.

Access Controls

Access controls are designed to limit or detect access to computer programs, data, equipment, and facilities to protect these resources from unauthorized modification, disclosure, loss, or impairment. Such controls include logical and physical security controls.

Logical security control measures involve the use of computer hardware and security software programs to prevent or detect unauthorized access by requiring users to input unique user identifications (ID), passwords, or other identifiers that are linked to predetermined access privileges. Logical security controls restrict the access of legitimate users to the specific

systems, programs, and files they need to conduct their work, to prevent unauthorized users from gaining access to computing resources.

Physical security controls include locks, guards, badges, alarms, and similar measures (used alone or in combination) that help to safeguard computer facilities and resources from intentional or unintentional loss or impairment by limiting access to the buildings and rooms where they are housed.

Our review of FMS' access controls identified a number of weaknesses at all of the sites we visited. These weaknesses, many of which were included in our prior year report, included data centers that (1) had weak network security configurations that allowed us to identify user names and compromise the associated passwords, (2) granted excessive and powerful systems privileges to certain users who did not need such access, (3) did not manage the administration of certain passwords and user IDs effectively, (4) were not always applying security system parameters so as to provide optimum security or appropriate segregation of duties, and (5) were not effectively monitoring and controlling dial-in access to certain local area networks and the mainframe environments. For example:

- Certain servers were not configured to provide optimum security.
- Messages and data sent and received by the mainframe applications through the network were not encrypted, increasing the risk that malicious users could obtain user IDs and passwords to gain unauthorized access to computer resources or disrupt operations.
- Certain system programmers, computer operators, quality assurance personnel, and regional financial center personnel had the capability to read, add, delete, or modify sensitive production data, increasing the risk for unauthorized access to production data and source code or the disclosure of sensitive data.
- The dial-in access to the local area network and mainframe environments did not require a unique user ID and the related password was not changed frequently, thereby providing inadequate protection from unauthorized access by intruders.

Due to the sensitive nature of the internal network control weaknesses we identified, these issues are described in the separate Limited Official Use report issued to you on September 22, 2000.

In addition, physical security controls at five of the six sites we visited were not sufficient to control physical access to these centers. For example, we

found that certain production staff, terminated employees, vendors, and other individuals without justified business purposes had unrestricted access to computer facilities.

The risks created by these access control weaknesses were heightened because FMS was not adequately managing and monitoring user access activities. Program managers and security personnel did not consistently monitor and evaluate user access rights, security violations, and software security settings at many of the sites visited. Because of these identified access control weaknesses, FMS is also at risk that unauthorized activities, such as corruption of financial data, disclosure of sensitive data, or introduction of malicious programs or unauthorized modifications of software, will go undetected.

System Software

System software coordinates and helps control the input, processing, output, and data storage associated with all of the applications that run on a system. System software includes operating system software, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems. Controls over access to and modification of system software are essential to protect the overall integrity and reliability of information systems.

During our fiscal year 1999 audit, we found that the software library listings at one data center did not agree with the corresponding volume locations or indexes on the systems or contained obsolete or unneeded library members. Obsolete or unneeded library members increase the risk that standard security software could be bypassed to obtain access to restricted system functions. In addition, the use of such library members could cause unexpected operating results. We also found, as we reported in the prior year, that the settings for two logical partitions allow programs operating under the authorized program facility to bypass standard security software and access restricted operating functions. Further, we found at another data center that certain operating system, security, and user profile reports cannot be produced due to system limitations. Consequently, unauthorized access to the key application and system resources could occur and not be detected promptly.

Application Software Development and Change Controls

Controls over the design, development, and modification of application software help to ensure that all programs and program modifications are properly authorized, tested, and approved. Such controls also help prevent security features from being inadvertently or deliberately turned off and processing irregularities or malicious code from being introduced.

We found application software development and change control procedure weaknesses at three of the six FMS sites we visited. As we reported in the prior year, a significant weakness at most of the sites we visited was that policies and procedures over system design, development, and modification were not established, were inadequate, or were simply not being followed. Specifically,

- procedures for making changes to application and system software were not consistently followed, such as obtaining written authorizations prior to making the changes, independent testing of changes, or authorizing the migration of application software changes from the test environment to production, were not followed;
- adequate documentation was not maintained to provide evidence of compliance with established application software development and change control policies and procedures; and
- changes to the applications were tested in the production environment rather than a test environment.

Without other effective compensating controls in place, failure to clearly define and implement a disciplined approach to application software development and change controls may result in changes that are not tested, documented, or approved. FMS also runs a greater risk that software supporting its operations will not (1) produce reliable data, (2) execute transactions in accordance with applicable laws, regulations, and management policies, or (3) effectively meet operational needs.

Segregation of Duties

Another key control for safeguarding programs and data is to ensure that duties and responsibilities for authorizing, processing, recording, and reviewing data, as well as initiating, modifying, migrating, and testing of programs, are separated to reduce the risk that errors or fraud will occur and go undetected. Duties that should be appropriately segregated include applications and system programming and responsibilities for computer operations, security, and quality assurance. Policies outlining the supervision and assignment of responsibilities to groups and related individuals should be documented, communicated, and enforced.

We found that programmers at one data center had the ability to read, add, delete, or modify data in the production data files. In addition, certain individual users and system programmers had been assigned the ability to administer the access permissions of on-line transactions. Programmers or other inappropriate individuals having access to production data, production source code, or production batch processes not only results in an inadequate segregation of duties but significantly increases the risk for unauthorized or inappropriate changes to production data and source code or disclosure of sensitive data.

During our fiscal year 1999 audit, we also found that the process for updating job descriptions had not been formally defined at another data center. Lack of current and approved job descriptions increases the risk that employees may not fully understand their job responsibilities, which could result in an inadequate segregation of duties.

Service Continuity

An organization's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information that is maintained electronically. For this reason, organizations should have (1) established procedures for protecting information resources and minimizing the risk of unplanned interruptions and (2) plans for recovering critical operations should interruptions occur. A contingency or disaster recovery plan specifies emergency response, backup operations, and postdisaster recovery procedures to ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. It addresses how an organization will deal with a full range of contingencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plan also identifies essential business functions and ranks resources in order of criticality. To be most effective, a contingency plan should be periodically tested in disaster simulation exercises, and employees should be trained in and familiar with its use.

Because it is not cost-effective to provide the same level of continuity for all operations, it is important that organizations analyze relevant data and operations to determine which are the most critical and what resources are needed to recover and support them. As discussed in our May 1998 best practices guide, the criticality and sensitivity of various data and operations should be determined and prioritized based on an overall risk assessment of the entity's operations. Factors to be considered include the importance and sensitivity of the data and other organizational assets

handled or protected by the individual operations and the cost of not restoring data or operations promptly.

In reviewing FMS' service continuity, we found that FMS management is still in the process of developing an entitywide service continuity plan. FMS has informed us that it is using its Year 2000 contingency plan as a starting point. Consequently, the FMS data centers are still at significant risk that in the event of an emergency or disaster, data center personnel may not be prepared to effectively prioritize recovery activities, integrate recovery steps in an effective manner, or fully recover systems.

FMFIA Reporting

FMFIA requires ongoing evaluations of the internal control and accounting systems that protect federal programs against fraud, waste, abuse, and mismanagement. It further requires that the heads of federal agencies report annually to the President and the Congress the condition of these controls and systems and on their actions to correct the weaknesses identified.

During the course of our work, we communicated our general computer control findings to FMS management. As a result, FMS reported its general computer control problems as a material weakness to the Department of the Treasury. The Department of the Treasury reported in its Fiscal Year 1999 Accountability Report that FMS, along with other Treasury components, had a material weakness in general computer controls designed to safeguard data, protect computer application programs, protect system software from unauthorized access, and ensure continued computer operations.

FMS' Application Controls Can Be Strengthened

Application controls relate directly to the individual computer programs, which are used to perform certain types of work, such as generating payments or recording transactions in a general ledger. In an effective general control environment, application controls help to further ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.

Authorization Controls

Authorization controls for specific applications, similar to general access controls, should be established to (1) ensure individual accountability and proper segregation of duties, (2) ensure that only authorized transactions

are entered into the application and processed by the computer, (3) limit the processing privileges of individuals, and (4) prevent and detect inappropriate or unauthorized activities.

Our follow-up review of FMS' authorization controls found that a number of weaknesses discussed in our fiscal year 1998 report continued. These weaknesses included

- incomplete, missing, or unapproved user application request forms;
- inappropriate access to application functions and privileges that were not required by the users' job responsibilities and that in some instances, also created an inadequate segregation of duties;
- terminated or dormant user IDs remained in the application security tables;
- users sharing IDs or being assigned multiple IDs without functional requirements;
- security reports not being consistently monitored or followed up on; and
- application passwords not being properly managed.

During our fiscal year 1999 testing of one key application, we found that documentation of the application that would normally be a part of an application's policies and procedures was not available for review. In addition, we found that application operators were not required to obtain approval by another operator or supervisor to continue processing when the application was out of balance.

The authorization control weaknesses described above increase the risk of unauthorized activities such as inappropriate processing of transactions, unauthorized access or disclosure of sensitive data, corruption of financial data, or disruption of operations.

Completeness Controls

Completeness controls are designed to ensure that all transactions are processed and missing transactions are identified. Common completeness controls include the use of record counts and control totals, computer sequence checking, computer matching of transaction data with data in a master or suspense file, and checking of reports for transaction data.

As discussed in our fiscal year 1998 report, our fiscal year 1999 review of completeness controls over one key FMS financial application found that there were no automated record counts and control totals to ensure that

data transferred from one application to another application were complete.

FRB Computer Controls Can Be Improved

Because the FRBs are integral to the operations of FMS, we assessed the effectiveness of general and application controls that support key FMS financial systems maintained and operated by the FRBs. Overall, we found that the FRBs had implemented effective general and application controls. Our fiscal year 1999 audit procedures identified certain new vulnerabilities in general controls that do not pose significant risks to the FMS financial systems, but nonetheless warrant FRB management's attention and action. These include vulnerabilities in general controls over (1) the entitywide security management program, (2) access to data, programs, and computing resources, and (3) system software. We also found vulnerabilities in authorization controls over two key applications. Our follow-up work found that the FRBs had corrected or mitigated the risks associated with most of the vulnerabilities that were identified in our prior year report and that work is in progress to address the remaining vulnerabilities. We provided details of these matters in a separate report to the Board of Governors of the Federal Reserve System along with our recommendations for improvement. FRB management has informed us that the FRBs have taken or plan to take corrective actions to address the vulnerabilities we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 2000 financial statements.

Conclusion

The pervasiveness of the computer control weaknesses—both old and new—at FMS and its contractor data centers place sensitive data and billions of dollars of payments and collections at risk of fraud. The severity of these risks magnifies as FMS expands its networked environment through the migration of its financial applications from mainframes to client-server environments. Thus, as FMS provides users greater and easier access to larger amounts of data and system resources, well-designed and effective general and application controls are essential if FMS' operations and computer resources are to be properly protected. It will take a significant and sustained commitment by FMS' management to fully address its serious computer control weaknesses, including establishing an effective entitywide computer security control program.

Recommendations

In our September 22, 2000, Limited Official Use version of this report, we reaffirmed our prior year recommendation that the Secretary of the Treasury direct the Commissioner of the Financial Management Service, along with the Assistant Commissioner for Information Resources, to establish an effective entitywide security management program.

In addition, we recommended that the Secretary of the Treasury direct the Commissioner of the Financial Management Service, along with the Assistant Commissioner for Information Resources, to correct each individual weakness that we identified and address each of the 59 specific recommendations detailed in that report.

Further, we recommended that the Secretary of the Treasury direct the Commissioner of the Financial Management Service, along with the Assistant Commissioner for Information Resources, to work with the FRBs to monitor corrective actions taken to resolve the computer control vulnerabilities related to FMS systems supported by the FRBs that we identified and communicated to the FRBs.

Agency Comments

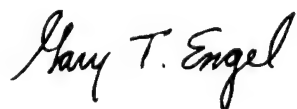
In commenting on a draft of this report, FMS stated that it recognizes that general and application security controls must continue to be improved. FMS also stated that it has made progress in correcting or mitigating the risks associated with many of the weaknesses we identified and that corrective actions are underway on the remaining findings. Further, FMS stated that it has taken and will continue to take action to heighten management focus on security as well as to institute a more systematic and comprehensive security management program. We will follow up on these matters during our audit of the federal government's fiscal year 2000 financial statements. In addition to its written comments, the staff of FMS provided technical comments, which have been incorporated as appropriate.

We are sending copies of this report to Senator Robert C. Byrd, Senator Ben Nighthorse Campbell, Senator Pete V. Domenici, Senator Byron L. Dorgan, Senator Frank R. Lautenberg, Senator Joseph Lieberman, Senator Daniel Patrick Moynihan, Senator William V. Roth, Jr., Senator Ted Stevens, Senator Fred Thompson, and to Representative Bill Archer, Representative Spencer Bachus, Representative Dan Burton, Representative Stephen Horn, Representative Steny H. Hoyer, Representative John R. Kasich,

Representative Jim Kolbe, Representative David R. Obey, Representative Charles B. Rangel, Representative John M. Spratt, Jr., Representative Jim Turner, Representative Henry A. Waxman, and Representative C.W. Bill Young in their capacities as Chairmen or Ranking Minority Members of Senate or House Committees and Subcommittees. We are also sending copies of this report to Richard L. Gregg, Commissioner, Financial Management Service; the Honorable Jeffrey Rush, Jr., Inspector General, Department of the Treasury; the Honorable Jacob Lew, Director, Office of Management and Budget; and other officials. Copies will also be made available to others upon request.

If you have any questions regarding this report, please contact me at (202) 512-3406. Key contributors to this assignment were Paula M. Rascona and Christine Robertson.

Sincerely yours,



Gary T. Engel
Associate Director
Governmentwide Accounting and
Financial Management Issues

Scope and Methodology

We used a risk-based and rotation approach for testing general and application controls. Under that methodology, every 3 years each data center and key application is subjected to a full scope review that includes testing in all of the computer control areas defined in FISCAM. During the interim years, we focus our testing on the FISCAM areas that we have determined to be at greater risk for computer control weaknesses.

The scope of our work for fiscal year 1999 included follow-up on weaknesses discussed in our fiscal year 1998 report and

- a focused review at one data center of the four general control areas intended to
 - protect data, files, and programs from unauthorized access, modification, and destruction;
 - limit and monitor access to system software programs and files that control computer hardware and secure applications;
 - prevent the introduction of unauthorized changes to systems and applications software; and
 - prevent any one individual from controlling key aspects of computer-related operations;
- a focused review at a second data center of the three general control areas intended to
 - protect data, files, and programs from unauthorized access, modification, and destruction;
 - prevent the introduction of unauthorized changes to systems and applications software; and
 - prevent any one individual from controlling key aspects of computer-related operations;
- a focused review at another data center of the two general control areas intended to
 - protect data, files, and programs from unauthorized access, modification, and destruction and
 - limit and monitor access to system software programs and files that control computer hardware and secure applications;
- a focused review at a fourth data center of the two general control areas intended to
 - prevent any one individual from controlling key aspects of computer-related operations and
 - ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption; and
- a focused review at a fifth data center of the two general control areas intended to

- protect data, files, and programs from unauthorized access, modification, and destruction and
- prevent any one individual from controlling key aspects of computer-related operations.

We limited our work at the sixth data center to a follow-up review of the status of weaknesses discussed in our fiscal year 1998 report.

We performed full scope application control reviews of two key applications to determine whether the applications are designed to ensure that

- access privileges (1) establish individual accountability and proper segregation of duties, (2) limit the processing privileges of individuals, and (3) prevent and detect inappropriate or unauthorized activities;
- data are authorized, converted to an automated form, and entered into the application accurately, completely, and promptly;
- data are properly processed by the computer and files are updated correctly;
- erroneous data are captured, reported, investigated, and corrected; and
- files and reports generated by the application represent transactions that actually occurred and accurately reflect the results of processing, and reports are controlled and distributed to the authorized users.

We limited our work over another seven key applications to a follow-up review of the status of weaknesses discussed in our fiscal year 1998 report.

To evaluate the general and application controls, we identified and reviewed FMS' information system general and application control policies and procedures; observed controls in operation; conducted tests of controls, which in some instances included selecting items using a method where the results are not projectable to the population; and held discussions with officials at selected FMS data centers to determine whether controls were in place, adequately designed, and operating effectively. We performed penetration testing at four data centers. Through our internal and external penetration testing, we attempted to access sensitive data and programs. These attempts were performed with the knowledge and cooperation of certain FMS officials.

Because the FRBs are integral to the operations of FMS, we followed up on the status of the FRBs' corrective actions to address vulnerabilities discussed in our fiscal year 1998 report. We assessed general controls over

Appendix I
Scope and Methodology

FMS systems that the FRBs maintain and operate and evaluated application controls over five key FMS financial applications.

To assist in our evaluation and testing of computer controls, we contracted with the independent public accounting firm PricewaterhouseCoopers, LLP. We determined the scope of our contractor's audit work, monitored its progress, and reviewed the related working papers to ensure that the resulting findings were adequately supported.

During the course of our work, we communicated our findings to FMS management, which informed us that the FMS has taken or plans to take corrective actions to address the weaknesses we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 2000 financial statements. We performed our work in accordance with generally accepted government auditing standards from July 1999 through February 2000. We requested comments on a draft of this report from the Department of the Treasury. Its comments are discussed in the "Agency Comments" section of this report and reprinted in appendix II.

Comments From the Financial Management Service



DEPARTMENT OF THE TREASURY
FINANCIAL MANAGEMENT SERVICE
WASHINGTON, D.C. 20227

September 7, 2000

Mr. Jeffrey C. Steinhoff
Assistant Comptroller General
United States General Accounting Office
Washington, DC 20548

Dear Mr. Steinhoff:

We appreciate the opportunity to comment on the draft General Accounting Office (GAO) Audit Report associated with the Financial Report of the United States Government, dated August 24, 2000, assessing the Financial Management Service's (FMS) general computer and application controls over key financial systems. The audit report presents the results of Fiscal Year (FY) 1999 tests of the effectiveness of controls, as well as the status of corrective actions resulting from GAO's FY 1998 audit. The report covers diverse computer environments at three FMS-operated sites, the Federal Reserve and four financial agent and contractor-operated sites. It represents a snapshot of FMS' security program and controls from almost twelve months ago – a time when we were focusing and dedicating resources and management attention to completing our Year 2000 (Y2K) efforts. Given the time that has passed since the end of FY 1999, the period covered by your report, many of the findings have already been corrected. As a result, the report does not reflect all of the controls currently in place at FMS.

FMS recognizes that general computer and application security controls must continue to be improved from a programmatic standpoint; however, many specific corrective actions have been taken to resolve the problems identified in the FY 1998 and FY 1999 audits, thereby reducing the associated risks. FMS has corrected or mitigated the risk associated with 80 of the 94 findings from the 1998 audit and ten of the 19 new findings identified in the 1999 audit. Corrective action is underway on all of the remaining 23 findings.

FMS has made considerable progress in strengthening its general computer and application controls by converting the payment processing systems to operate under the Multiple Virtual Storage (MVS) operating system as part of our Y2K program. This activity in itself corrected ten of the outstanding findings. Considerable improvement in controlling system access on our major computing platform has been made through the implementation of a centralized automated access control system. This access control system provides an audit trail of all system access requests and requires the electronic approval of the access requests by management prior to access being granted. We have also re-certified system users and those having physical access to our primary data center, and we have made significant progress in establishing and testing our disaster recovery program for payment processing.

FMS has taken and will continue to take action to heighten management focus on security, as well as to institute a more systematic and comprehensive security

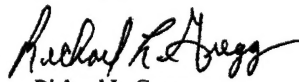
Appendix II
Comments From the Financial Management
Service

Page 2 – Mr. Jeffrey C. Steinhoff

management program. To achieve this goal, we have revised and issued new information technology security policies and we are implementing a more effective system certification and accreditation program. We will also ensure that security is a key management issue for all new system development efforts. To further ensure that adequate controls are in place, we have implemented a rigorous management control program to closely track the status of corrective actions, conduct verification reviews and provide monthly briefings to senior FMS management.

Although we have not completed all of the actions necessary to address all issues related to our entity-wide security program, we have made steady progress. This is demonstrated by the significant decline in the number of findings this past year. I can assure you that computer security remains one of FMS' top priorities and progress will continue to be made to ensure the integrity, confidentiality and availability of our key financial systems.

Sincerely,



Richard L. Gregg

cc: D. Hammond

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are \$2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet:
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web home page at:

<http://www.gao.gov>

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- Web site: <http://www.gao.gov/fraudnet/fraudnet.htm>
- e-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)

Appendix II
Comments From the Financial Management
Service
